SPECIFICATION AMENDMENTS

On page 4, replace the paragraph at lines 12-24 with the following paragraph:

In order to reduce the risk of unauthorized copying of copyrighted works, several companies, including Hitachi, Ltd., Sony; Intel, and others have proposed an industry standard for digital consumer electronics devices which involves the use of authentication and key exchange procedures along with data encryption and the use of a digital communication bus which complies with IEEE standard 1394. The bus is sometimes referred to as "1394 Firewire", The proposed standard, hereinafter .referred to as the "5C Standard", is discussed in the 5C Digital Transmission Content Protection White Paper ~~White Paper~~, Revision 1.0, dated July 14, 1998.

On page 6, please replace the paragraphs at lines 1-24 with the following:

In this system, authentication messages, system renewal messages, authentication keys, exchange keys and session keys, in addition to encrypted data, are passed between the system i00 and other devices via the bus 122. Interface 118 is responsible for electrically interfacing between bus 122 and system elements, such as authentication and key exchange subsystem 116 content cipher

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

subsystem 120. The authentication and key exchange subsystem <u>116</u> receives and exchanges, via bus 122, authentication and key information as well as system renewal messages. The content cipher subsystem <u>120</u> is responsible for encrypting video information prior to transmission and decoding received encrypted •information using content keys provided by authentication and key exchange system 116, to the cipher subsystem <u>120</u>.

Storage 112 stores un-encrypted video data, copyright status and system renewal information.. The system renewal and copyright status information is provided to authentication and key exchange subsystem 116. The video residing in the storage device 112 is supplied to, or received from, the content cipher subsystem <u>120</u> which is responsible for encoding/decoding video information passed over bus 122.

On page 15, please replace the paragraphs from line 1-25 with the following paragraphs:

Fig. 9 ~~illustrates the steps performed by a video signal encryption circuit in accordance with one exemplary embodiment of the present invention~~ <u>is omitted and thus not described herein</u>.

Fig. 10 illustrates a display device capable of decrypting and displaying video signals generated by the display adapter of Fig. 8.

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

Fig. 11 ~~illustrates the steps performed by a video signal decryption circuit in accordance with one exemplary embodiment of the present invention~~ is omitted and thus not described herein.

Fig. 12 illustrates a value mapping circuit of the present invention.

Fig. 13 ~~illustrates an encryption circuit suitable for use in the display adapter illustrated in Fig. 8~~ is omitted and thus not described herein.

Fig. 14 ~~illustrates a video signal decryption circuit suitable for use in the display device illustrated in Fig. 10~~ is omitted and thus not described herein.

Fig. 15 illustrates a MUX suitable for use in the value mapping circuit illustrated in Fig. 12.

On pages 17-18, please replace the paragraph starting at line 13 on page 17 with the following:

System 200 includes general purpose computing device 220 taking the form of, e.g., a PC. PC ~~200~~ 220 may include processing unit 221, system memory 222 and system bus 223 that couples various system components including the system memory to Processing unit 221. System bus 223may be any of several types of bus structures including memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory may include read only memory

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

(ROM) 224 and/or random access memory (RAM) 225. Basic input/output system 226 (BiOS), including basic routines that transfer information between elements within PC 220, such as during start-up, may be stored in ROM 224. PC ~~200~~ 220 may also include hard disk drive 227 for reading from and writing to a hard disk (not shown), magnetic disk drive 228 for reading from or writing to (e.g., removable) magnetic disk 229 and optical disk drive 230 for reading from or writing to removable (magneto) optical disk 231, such as a compact disk or other (magneto) optical media. Hard disk drive 227, magnetic disk drive 228 and (magneto) optical disk drive 230 may be coupled with system bus 223 through hard disk drive interface 232, magnetic disk drive interface 233 and a (magneto) optical drive interface 234, respectively. The drives and their associated storage media provide nonvolatile storage of machine readable instructions, data structures, program modules and other data, e.g., video data. Although the exemplary environment described herein employs a hard disk, a removable magnetic disk and a removable optical disk, those skilled in the art will appreciate that other types of storage media, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories (RAMs), read only memories (ROM), and the like may be used .instead of, or in addition to,~ the storage devices introduced above.

421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

On pages 18-19, please replace the paragraph starting at line 19 on page 18 with the following:

A number of program modules may be stored on hard disk 223, magnetic disc 229, (magneto) optical disk 231, R0M 224 or RAM 225, such as, e.g., operating system 235, one or more application programs 236, other program modules 237 and/or program data 238. A user may enter commands and information into PC 220 through input devices, such as, e.g., keyboard 240 and pointing device 242. Other input devices (not shown) such as a microphone, joystick, game pad, satellite dish, Scanner, or the like may also be included. These and other input devices are often connected to the processing unit through serial port interface 246 coupled to the system bus 223. However, input devices may be connected by other interfaces, such as a parallel port, a game port or a universal serial bus (USB) -- all of which are not shown.

On page 19, please replace the paragraph starting at line 4 with the following:

A display device, e.g., monitor 247, implemented in accordance with the present invention is connected to system bus 223 via an interface, such as inventive display adapter 248. In addition to being coupled to monitor 247 and system bus 223, display adapter 248 is coupled to external DVD player 251 via IEEE 1394 standard digital data bus, e.g., 1394 Firewire 249. Video

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

adapter ~~248~~ 223 can receive encoded video via bus 249 or unencoded video via, e.g., system bus 248. Bus 249 connects video adapter 248 directly to 5C Standard compliant CE devices without having to pass encrypted information from a CE device through other computer system components.

On page 19, please replace the paragraphs starting at line 24 with the following:

In addition to monitor 247, PC 220 may include other peripheral output devices (not shown), such as, e.g., ~~speakers and~~ printers. PC 220 may include a sound card 261 and speakers 261.

PC 220 may operate in a networked environment which defines logical connections to one or more remote computers, such as remote computer 259. Remote computer 259 may be another PC, a server, a router, a network computer, a peer device or other common network node, and may include many or all of the elements described above relative to PC 220~~, although only memory storage device 250 has been illustrated in FIG. 2~~. The logical connections depicted in this figure include local area network (LAN) 251 and wide area network (WAN) 252, which may comprise, e.g., an intranet and Internet, respectively.

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

On page 25, please replace the paragraph starting at line 9 with the following:

I/O interface 402 serves to couple 1394 content ciphers subsystem 414 to video processor 404 and system bus 223. Decoded video output produced by content cipher subsystem 414, copy restrictions permitting, can be transmitted over system bus 223 or processed by video processor 404. Video data processed by video processor 404 can be applied to a display via the ~~digital matrix multiplier~~ video signal encryption circuit 406 and second I/O interface 412..

On page 29, please replace the paragraph starting at line 5 with the following:

In one relatively simple embodiment, the video signal encryption circuit 406 swaps, as a function of the pseudo-random number generator 410 output, the R, G, and B video signals to generate video signals R', G' and B'. Here, the signals on lines 430, specifically 430a, 430b and 430c, represent signals generated by switching the input to each line so that at any given time it is difficult to determine which of these three lines is being used to transmit the R, G, and B video signals. In such an embodiment, the R, G and B signals between the display adapter and monitor are pseudo-randomly swapped on a line-by-line basis. A session key, exchanged with the display device is used to drive pseudo-random number generator 410. since the session key and pseudorandom

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

number generation techniques are common to both the display adapter and display device, the display device can perform the inverse swapping operation to properly reconstruct the R, G and B video signals.

On page 33, please replace the paragraph starting at line 22 with the following:

As discussed above, to eliminate a need for an inversion circuit and/or matrix inversion operation, self-inverting matrices may be used. FIG. 7 illustrates a matrix multiplication operation that may be performed by the video signal encryption circuit 406 to encrypt R, G and B video signals. Reference numeral 602 indicates a self-inverse matrix that can be used to encrypt R, G, and B signals.

On page 34, please replace the paragraphs from lines 5-31 with the following:

For decoding to accurately occur, display adapter 248 and display device 247 need to be synchronized such that the correct session key is used for decoding each line of both transmitted and received video images. Synchronization Should occur promptly after loss of synchronization, e.g., due to loss of power or a noise signal. One approach to maintaining synchronization is to periodically establish a new session key, e.g.., every few seconds, e.g., 5 seconds.

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

In the event display device 247 loses power, this display device 247 can signal the display adapter 248 via one of plug and play lines 312 to establish a new session key.

Alternatively, the display device 247 can actively monitor and detect loss of adapter/display synchronization. Specifically, the display adapter 248 transmits a frame counter value to the display device 247 during each vertical blanking period. The display device maintains its own count of received frames which it then compares to a value provided by display adapter 248. If a is match between the frame count provided by the display adapter 248 and that maintained in the display device is detected by the latter, the display device 247 signals the display adapter 248 to initiate a re-synchronization operation.

On page 36, please replace the paragraph starting at line 20 with the following:

The session key established by the authentication and key exchange system 516 serves as input to pseudo-random number generator 510. The output of the pseudo-random number generator 510 is used by the video signal decryption circuit 506 in. performing a decryption operation. The pseudo-random number generator output represents matrix coefficients Which are used as part of a matrix multiplication operation performed by video signal decryption circuit 506. Hence, a session key drives the pseudo-random number

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

generators, used for encrypting and decrypting, in display adapter 248 and display 247, respectively.

On page 44, please replace the paragraph starting at line 14 with the following:

Fig. 10 illustrates a display device 947 which is capable of receiving and decrypting the R', G' B' encrypted analog video signals generated by display adapter 848. The display device 947 includes many components which are the same as, or similar to, those previously discussed with regard to Fig. 6. Such components are identified in Fig. 10 using the same reference numerals as used in Fig. 6 and will not be described again in detail. Note that the display device 947 includes a pseudo random number generator 810 and video signal decryption circuit 906 ~~encryption circuit 806~~ which perform similar functions to those of the like named Fig. 6 components.

Due to implementation issues relating to the decryption circuit 906, and the differences in the implemented analog signal encryption between the Fig. 6 and Fig. 10 embodiments, these circuits may be implemented using hardware and/or software that differs from that used to implement the like named circuits found in Fig. 6.

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

On page 42, please replace the paragraph starting at line 11 with the following:

The steps 700~~,~~ are performed by the video signal encryption circuit 806, to encrypt R, G, B video signals as a function of the mapped set A of permutation matrix values~~, are shown in Fig. 9~~.

Please replace the paragraphs starting at line 27 of page 54 through page 58, line 22 with the following paragraphs:

~~An~~ The following describes an encryption circuit 806 suitable for use as the encryption circuit of Fig. 8 ~~is illustrated in Fig. 13~~. ~~As illustrated, the~~ This suitable encryption circuit ~~806~~ includes first through third signal encryption modules ~~1109, 1111, 1113~~ which are responsible for generating the R', G' and B' encrypted analog signals, respectively. Each of the first through third encryption modules includes first, second and third analog multipliers ~~1110, 1112, 1114,~~ and an analog adder ~~1116~~. The gain of the first through third analog multipliers ~~1110, 1112, 1114~~ in each of the encryption modules is controlled by a corresponding mapped permutation matrix value. The values used to control the first through third adders of the first encryption module ~~1109~~ are the values $[A1_1, A1_2, A1_3]$ which form the first row A1 of the mapped permutation matrix A. The values used to control the first through third adders of the second encryption module ~~1111~~ are the values $[A2_1, A2_2, A2_3]$ which form the second row A2 of the mapped permutation matrix A. The values

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

used to control the first through third adders of the third encryption module ~~1113~~ are the values [$A3_1$, $A3_2$, $A3_3$] which form the third row A3 of the mapped permutation matrix A.

The signals output by a decryption module's first through third analog multipliers ~~1110, 1112, 1114~~ are summed by the analog adder ~~1116~~. In this manner, the encrypted analog video signal R' is generated by the first encryption module ~~1109~~, the encrypted analog video signal G' is generated by the second encryption module 1111, and the encrypted analog video signal B' is generated by the third encryption module ~~1113~~.

The following describes a ~~A~~ video signal decryption circuit 906 suitable for use in the display device 947 ~~is illustrated in Fig. 14~~. As illustrated, the video signal decryption circuit ~~906~~ includes first, second and third decryption modules ~~1201, 1203, 1205~~ each of which is responsible for enerating one of the decoded analog R, G, B video signals. Which particular decryption module ~~1201, 1203 or 1205~~ will generate the R, G, or B signal at any given time will depend on the mapped permutation matrix A.

Each of the first through third decryption modules ~~1201, 1203, 1205~~ processes a different pair of encrypted R', G', B' analog video signal to generate a decrypted analog video signal therefrom. The first decryption module ~~1201~~ processes the pair of encrypted signals (R', G'), the second decryption module ~~1201~~ processes the pair of encrypted signals (G', B'), while the third decryption module ~~1205~~ processes the pair of encrypted signals (B', R').

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

The decryption modules ~~1201, 1203, 1205~~ each include an analog adder and divider circuit ~~1202~~, first through third pass gates ~~1220, 1222, 1224~~ and an output control circuit ~~1210~~. The analog adder and divider circuit ~~1202~~ receives as its input the two encrypted video signals to be processed. If a variable α is supported, then the circuit ~~1202~~ also receives an α value to be used. In cases where α is fixed, e.g., at 1, the α input is not required. The circuit ~~1202~~ generates a decrypted analog video signal by summing the two encrypted input signals and dividing by 2 α . The decoded video signal is supplied to the input of each of the three pass gates ~~1220, 1222, 1224~~.

The first pass gate ~~1220~~ of each decryption module is coupled to the R signal output line, the second pass gate ~~1222~~ of each decryption module is coupled to the G signal output line, while the third pass gate ~~1224~~ of each decryption module is coupled to the B signal output line. Each pass gate ~~1220, 1222, 1224~~ passes an input signal when a 1 is supplied to the control input of the pass gate, and blocks the input signal when a 0 is supplied to the control input of the pass gate. Thus, by controlling the pass gates ~~1220, 1222, 1224~~ the decrypted video signal generated by any one of the first, second or third decryption modules ~~1201, 1203, 1205~~ can be output on any one of the R, G, or B signal lines.

The control circuit ~~1210~~ of each decryption module determines to which R, G, or B output line the decrypted video signal produced by the module will be sent. The first, second and

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

third decryption modules ~~1201, 1203, 1205~~ are controlled so that they each output the decrypted video signal they produce to the correct one of the R, G, B video signal lines.

The output line for a video signal, generated from a particular encrypted signal pair, is determined by comparing the corresponding rows of values in the mapped permutation matrix and finding the column location where the values agree. The control circuit ~~1210~~ does this by performing a bit wise ANDing operation after negating mapped permutation values included in the two rows from the set A1, A2, A3, which correspond to the set of encoded signals being processed. Accordingly, the control circuit ~~1210~~ of the first decoder module ~~1201~~ performs a bit wise ANDing operation after negating permutation matrix values A1, A2. The control circuit ~~1210~~ of the second decoder module ~~1203~~ performs a bit wise ANDing operation on negated permutation matrix values A2, A3. Similarly, the control circuit ~~1210~~ of the third decoder module ~~1205~~ performs a bit wise ANDing operation on negated permutation matrix values A3, A1.

The ANDing operation performed by the control circuits ~~1210~~ produces a threebit control signal with a 1 located at the bit location where values in the two rows of the mapped permutation matrix being compared agree. The two other bits of the resulting 3 bit signal will be zero. The first through third bits generated by the control circuit ~~1210~~ are used to control, the first through third pass gates ~~1220, 1222, 1224~~ of the corresponding demodulator module. In this

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

manner, the decrypted video signal generated by the decryption modules is routed to the proper one of the R, G, B signal lines.

lee&hayes
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com